Stand Down
INFORMATION ASSURANCE (IA) TRAINING

Marine Corps Forces Europe

MARFOREUR
IA Chain

Designated Approving Authority – Col B. P. Kearney

AC/S G-6 – LtCol William E. Callahan

Information Assurance Manager – MSgt Alton Thompson

Information Assurance Officer – SSgt Jason Rahn

Information Assurance Technician – Sgt James Taylor

Marine Corps Forces Europe

INFORMATION ASSURANCE

OVERVIEW

- Information Assurance (What and Why)
- Objectives of the IA Program
- Your Role
- Passwords
- Internet Access and Email Use
- Data Storage
- Virus and Other Malicious Code
- Personal Electronic Devices (PEDS)
- SIPRNET (Classified Network)

INFORMATION ASSURANCE

What is Information Assurance?

- Basically any measure you use to protect your information from threats. This includes incorporating protection, detection, and reaction capabilities into information systems.

INFORMATION ASSURANCE

What is the Threat?

- Internal
  - Intentional (Disgruntled Employee)
  - Unintentional (Employee Error)
- External
  - Intentional (Terrorists, Hackers)
  - Unintentional (Natural Disaster)

Why Information Assurance?

- Provide:
  - Confidentiality: Does the person need to know
  - Integrity: Is the information accurate
  - Availability: Can the information be accessed when required
  - Authentication: Guarantees the identity of the person, computer, or information
  - Non-repudiation: Verifies the receipt of electronic transactions

Objectives of the IA Program

- Protect government information and resources from possible threats
- Conduct an assessment of threats, identify and apply appropriate safeguards
- Explain information assurance
- Protect computers from viruses
- Explain the user’s roles and responsibilities for IA

Your Role in Security

It is commonly assumed that someone else takes care of security, especially in the workplace, but YOU play a key role in IA.

INFORMATION ASSURANCE

Defense – In - Depth

- The Defense in Depth approach employs and integrates the abilities of people, operations, and technology to establish multi-layer and multidimensional protection.
- People (YOU) using technologies to conduct operations are the strategy’s central element.

PASSWORDS

- When using passwords here are some things you should consider:
  - Password should be at least 8 characters
  - You should use multiple character sets
  - Your password should not be found in the dictionary, not a family name, and does not have inherent meaning
  - Memorize your password, do not write it down

PASSWORDS

- Treat your password like a toothbrush
  - Use it daily
  - Change it often (At least every 90 days)
  - Don’t share with anyone

Internet Access and Email

- Official Use
  - Work Related
  - Support of your Mission
  - Enhance Professional Skills
  - Formal Academic Education
  - Professional Development Program

Internet Access and Email

- Authorized Use
  - Does not adversely affect your performance of duties
  - Serves as a public interest
  - Minimal frequency and duration
  - Does not overburden resources
  - No added cost to the Government
  - No adverse reflection on the Government

INFORMATION ASSURANCE

Internet Access and Email

- Prohibited Use
  - Illegal or malicious activities
    - Chain Letters
    - Unauthorized fund raising
    - Offensive or obscene material (Porno Material)
  - Political or religious activity
  - Financial Gain / Non-Organization Ads
  - Sharing Internet Accounts
  - Web Chat (yahoo, MSN)
  - File Sharing/Peer to Peer (Kazaa, PC Anywhere)
  - Streaming Media (i.e. radio stations, on-line MP3)
  - Yahoo & Hotmail, G-Mail, Black Planet, Date Service

Unauthorized Software

- Pirated software
- Peer-to-peer file sharing programs (i.e. Kazaa, PC anywhere)
- Internet relay chat (IRC) programs (i.e. Yahoo messenger)
- Network scanners/packet sniffing programs
- Hacking tools/malicious software
- Multimedia programs not included in set-up

INFORMATION ASSURANCE

Data

- Government computers and storage devices and media are for storage of government data. Personal data (data not relating directly to official U.S. Government business) will not be stored in MARFOREUR computers, peripherals, and communications devices

INFORMATION ASSURANCE

Data

- Government Data will not be stored on privately owned computers, peripherals nor Communication devices. It is strictly prohibited to view, store, or process Privacy Act Data and for Official Use Only (FOUO) data on privately owned systems.

Data

- File encryption will not be used on any MARFOREUR computer system except as authorized and configured by the IAM. The only email encryption system authorized for use on DoD computers is DoD PKI

INFORMATION ASSURANCE

Data

- **Data on the Shared “Headquarters” Drive**. This data is intended to be accessible by any user on the MARFOREUR network for purposes of collaboration. Therefore the default permissions set for every folder on this drive is “full control”, i.e. the ability to read, write, add, and delete files.

Data

- The shared storage on the Network drive is for storage of work related information. It is not a personal storage space for MP3, AVI nor pictures.

Malicious Code

- Malicious Code is code designed with the intent to deny, destroy, modify, or impede systems configuration, programs, data files, or routines
  - Viruses
  - Trojan Horses
    - Bombs
    - Worms

Viruses

- A virus is any self-replication, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence

How Do Viruses Spread

- Internet and E-Mail
- Sharing Software (Freeware or Shareware)
- Commercial Software
- Preformatted Disks and Hardware
- Third-party Use of Your Computer
- Internet Chat Rooms
- Running Contaminated Software from a Shared Source

Why are Viruses Successful

- Lack of Awareness
- Lack of Antivirus software
- Antivirus definitions are not up to date
- Bugs and Loopholes in System Software
- Unauthorized Use
- Network Misuse

Trojan Horses

- A Trojan Horse is a computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification, or destruction of data.

Trojan Horses

- Bombs
  - A program, generally malicious in nature, hidden within or acting as another program, that is designed to execute at a specific future time or event

Trojan Horses

- Worms
  - An independent program that copies itself from machine to machine across the network often shutting down networks and computer systems as it spreads

INFORMATION ASSURANCE

Guidelines to Prevent Infection

- Use current anti-viral software at ALL times
- Scan all diskettes regardless of source
- Scan transfer of information to/from computers
- Do not us shareware or peer to peer software
- Do not run computer games

INFORMATION ASSURANCE

Antivirus Software

- Antivirus Software **WILL** be on all DOD Computers
- Personal Computers at home are authorized to run the DOD Antivirus software
- Personal Computers that connect to Outlook Web Access are required to have Anti-virus software installed

INFORMATION ASSURANCE

What to Do If You Have Been Infected

- STOP all processing
- DO NOT turn off your computer
- Unplug your computer from the network
- Contact the G-6 helpdesk
- Collect all diskettes your computer has accessed

INFORMATION ASSURANCE

Personal Electronic Devices (PEDS)

- What are PEDS?
  - Palm Pilots, Palmtops
    - (Not used at MARFOREUR)
  - Black Berry
  - Hand-Held Computers- (not used at MarForEur)
  - Cell Phones
  - Two-Way Pagers – (not used at MarForEur)
  - Wireless E-Mail Devices - (not used at MarForEur)
  - Audio and Video Recording Devices

USB Devices (Thumb Drives)

- MarAdmin 450/03
  - States that ALL USB ports will be disabled on computing devices that process classified information. This is due to the inherent risk that they pose. If an USB port is needed then you must get approval in writing from the local DAA to have the USB activated.
  - Also states that any connection of personal removable secondary storage media (i.e. Thumb Drives, Flash Drive) to unclassified government computing device without prior written approval of the local DAA is **prohibited**.

INFORMATION ASSURANCE

- Personal Media
  - DVDs, CDs, diskettes and CDR/CDRW/DVDR from home
  - Digital Camera’s
  - MP3 Devices

Usage of Personal Media is strictly **PROHIBITED**

INFORMATION ASSURANCE

SIPRNET (Classified Network)

- Every user is responsible for safeguarding classified material
- Any individual who becomes aware of the loss, possible compromise, or compromise of classified information or material they will immediately notify the security manager. This includes knowledge that an unauthorized person has “borrowed” another users ID and password to gain access to the SIPRNET.

INFORMATION ASSURANCE

SIPRNET Accounts

- A SIPRNET Statement of Understanding (SOU) must be on file with the G-6 shop.
- SIPRNET accounts remain active for one year, after which the user must complete another SOU.
- An active SECRET or above security clearance is required to obtain a SIPRNET account.
- All high to low transfers from the SIPRNET to the unclassified network is to be executed by G-6 Information Assurance Personnel Only.

INFORMATION ASSURANCE

Secured Areas

- Maintain physical security at all times (window blinds, doors shut/locked etc…).
- Ensure all personnel read and understand the SIPRNET Standard Operating Procedures (SOP).
- Report changes to the SIPRNET area to the Information Assurance Manager in a timely manner.
- Follow all guidelines and policies as directed by the MFE 5239

Access List / Mailing List

- Are to be used for granting access instead of individual account names
- Are to be centrally managed and maintained
- Are to have the limited access
- Follow all guidelines and policies as directed by the MFE 5239

INFORMATION ASSURANCE

Outlook Web Access

- In order to get Outlook web access is limited to those whom have been identified as having that requirement.
- Ensure all personnel read, understand and sign the OWA user agreement.
- Verify that current anti-virus software is running on their home machine.
- Follow all guidelines and policies as directed by the MFE 5239

INFORMATION ASSURANCE

- You have completed the annual Information Assurance Training.